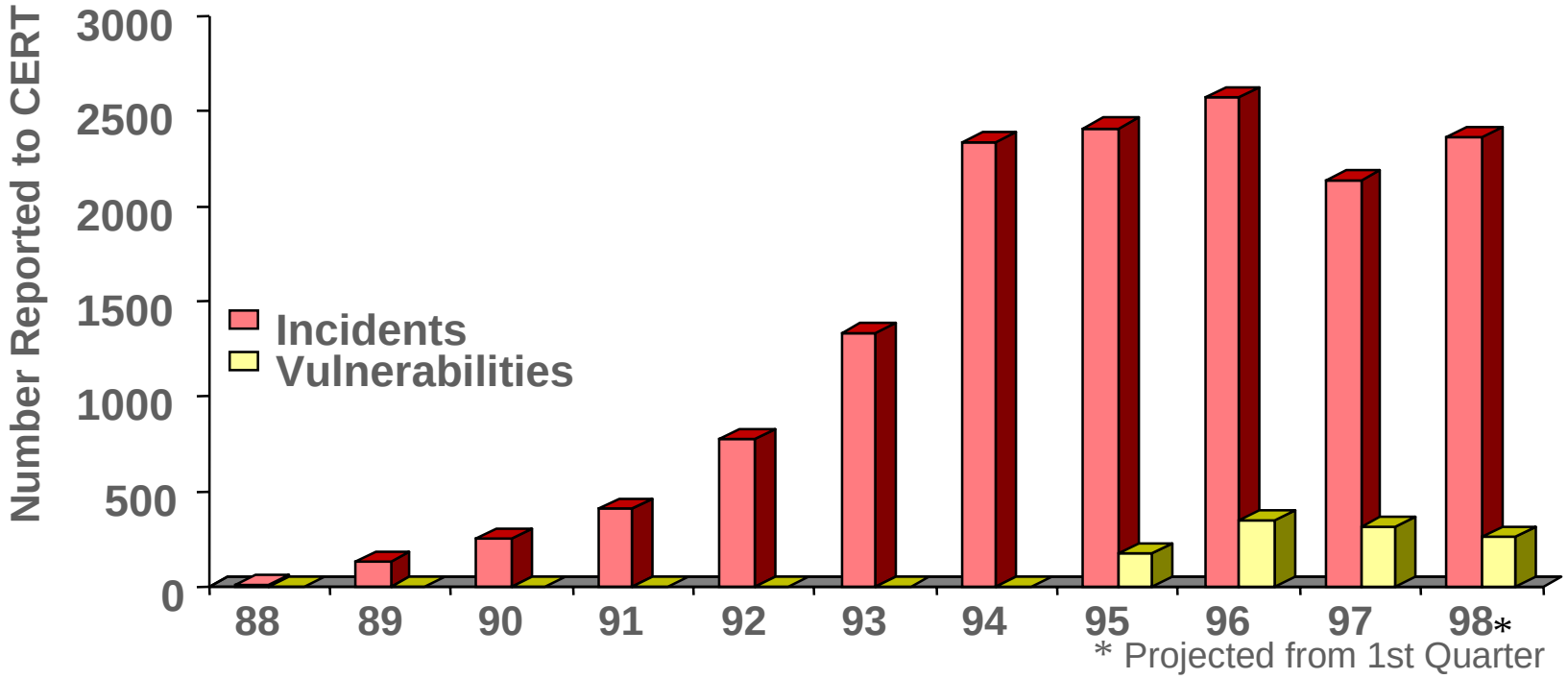
The Problem:

We are under attack!

- DISA estimates that there are 250,000 attacks on DoD computer systems every year
- Computer attacks against US systems are up 22% from 1996 to 1997, according to a survey by the Computer Security Institute and the FBI



Information Survivability
Background

DoD depends on information technology for information dominance, but

DoD systems are increasingly vulnerable to attack because:

- They are increasingly connected to one another and to civilian networks using Internet technology

  Vulnerabilities in this technology or in any connected system can be exploited by anyone in the world to penetrate and corrupt DoD systems

- There is increased use of COTS products

  Commercial security is not designed nor intended to withstand the IW attacks of concern to DoD

- DoD depends on commercial infrastructures such as the phone system

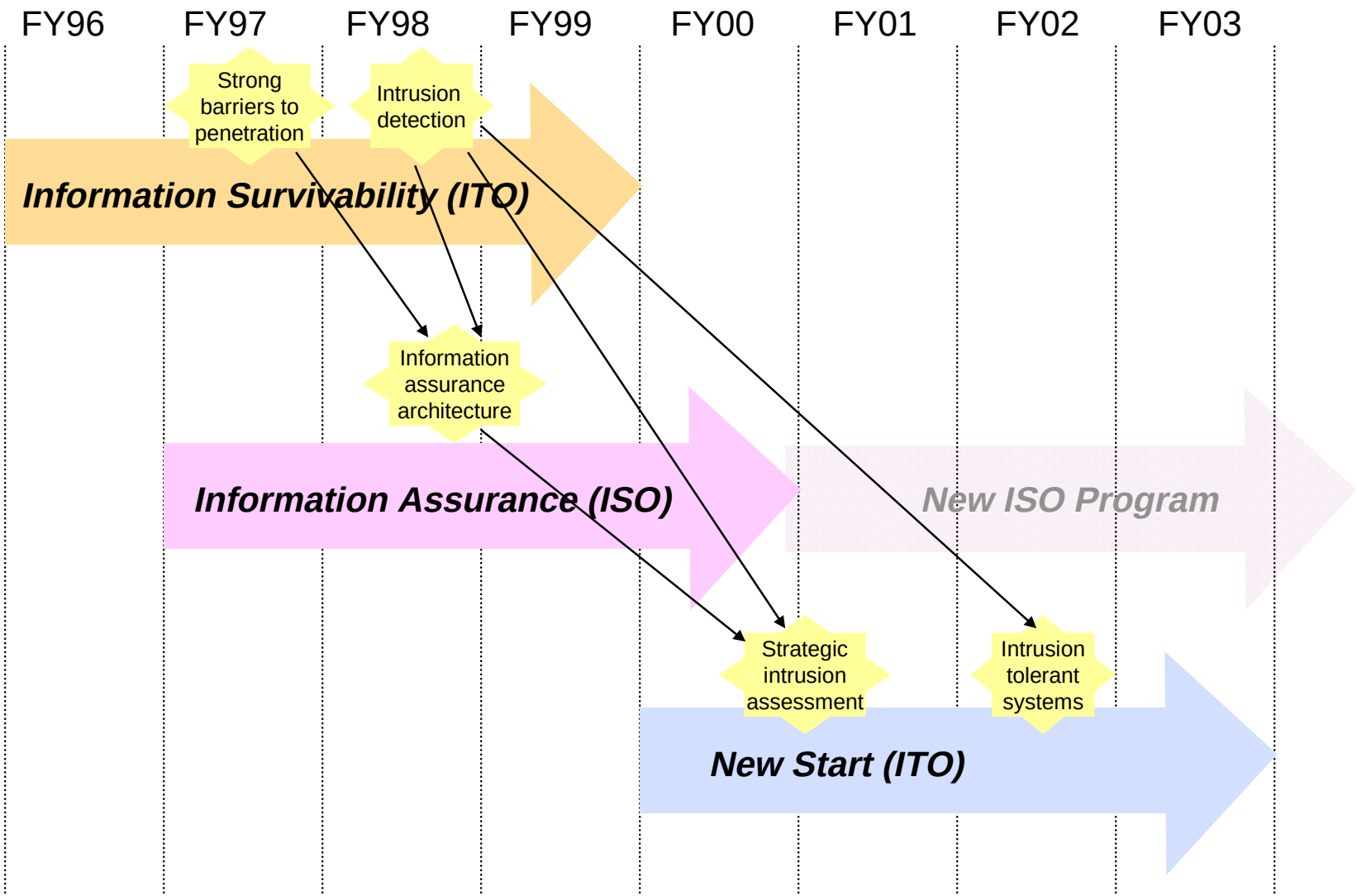
  These are vulnerable

DoD's past approaches did not succeed

Long-Term Strategy

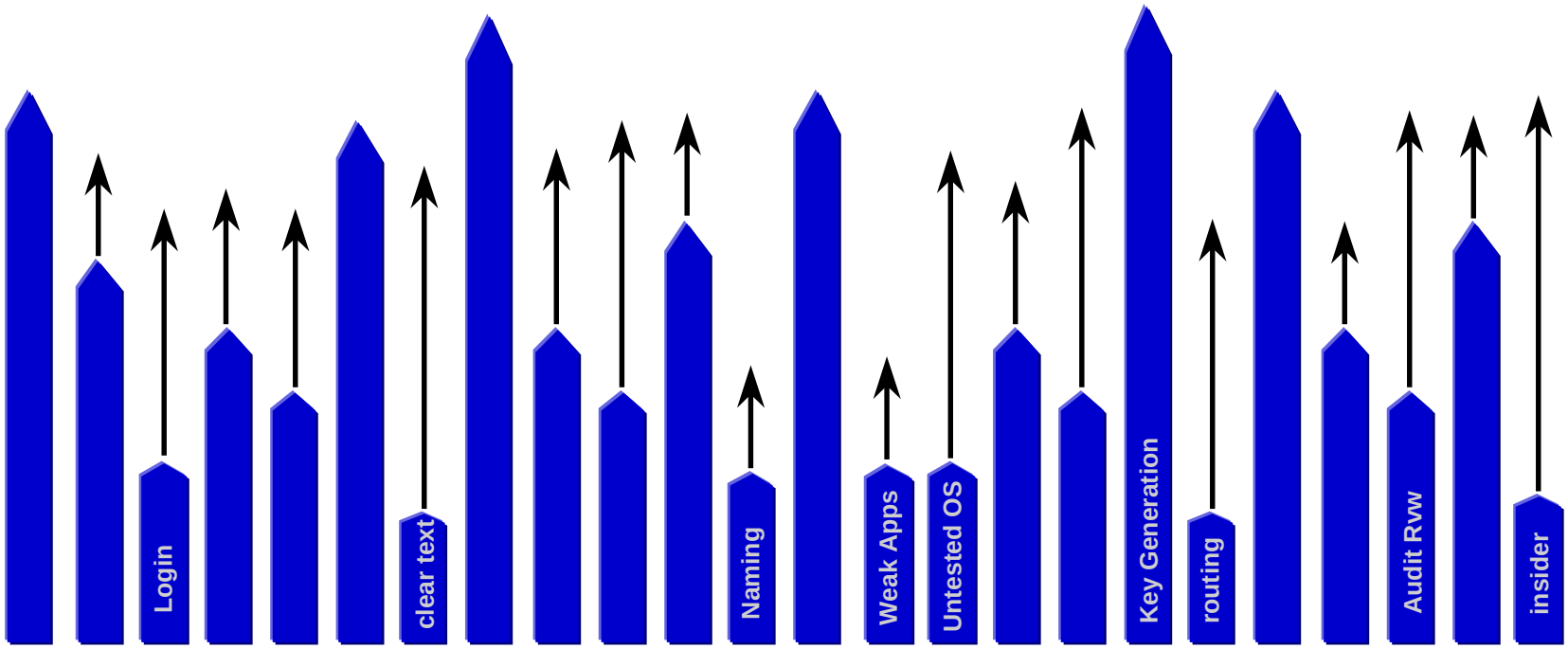
- Strong Barriers to Penetration
  - Hardened networks and software
- Intrusion Detection
  - Local capability
- Information Assurance Architecture
  - Integrate technologies into systems solutions
- Strategic Intrusion Assessment
  - Distinguish national scale attacks
- Intrusion Tolerant Systems (partially)
  - Maximize the residual capability

Roadmap


FY96
FY97
FY98
FY99
FY00
FY01
FY02
FY03
Strong barriers to penetration
Intrusion detection
Information Survivability (ITO)
Information assurance architecture
Information Assurance (ISO)
New ISO Program
Strategic intrusion assessment
Intrusion tolerant systems
New Start (ITO)

Barriers to Attack: Investment Strategy

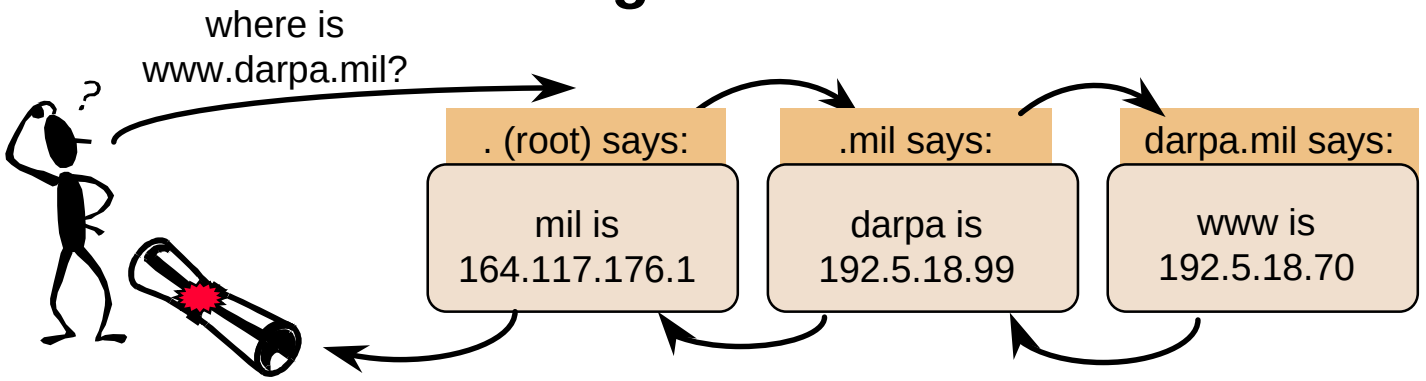
Balanced Protection



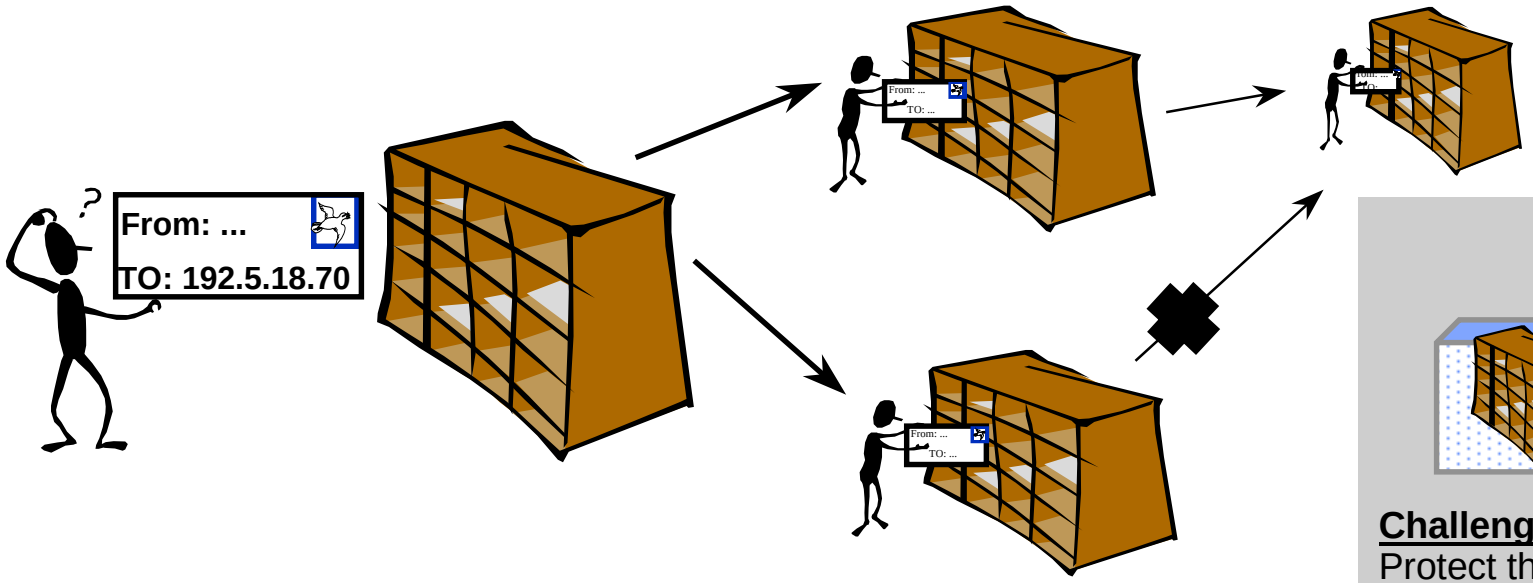
Protecting the Communications Infrastructure

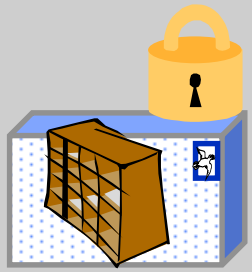
Barriers
Detection
Integration
Strategic Assessment
Intrusion tolerance

Securing Names and Addresses



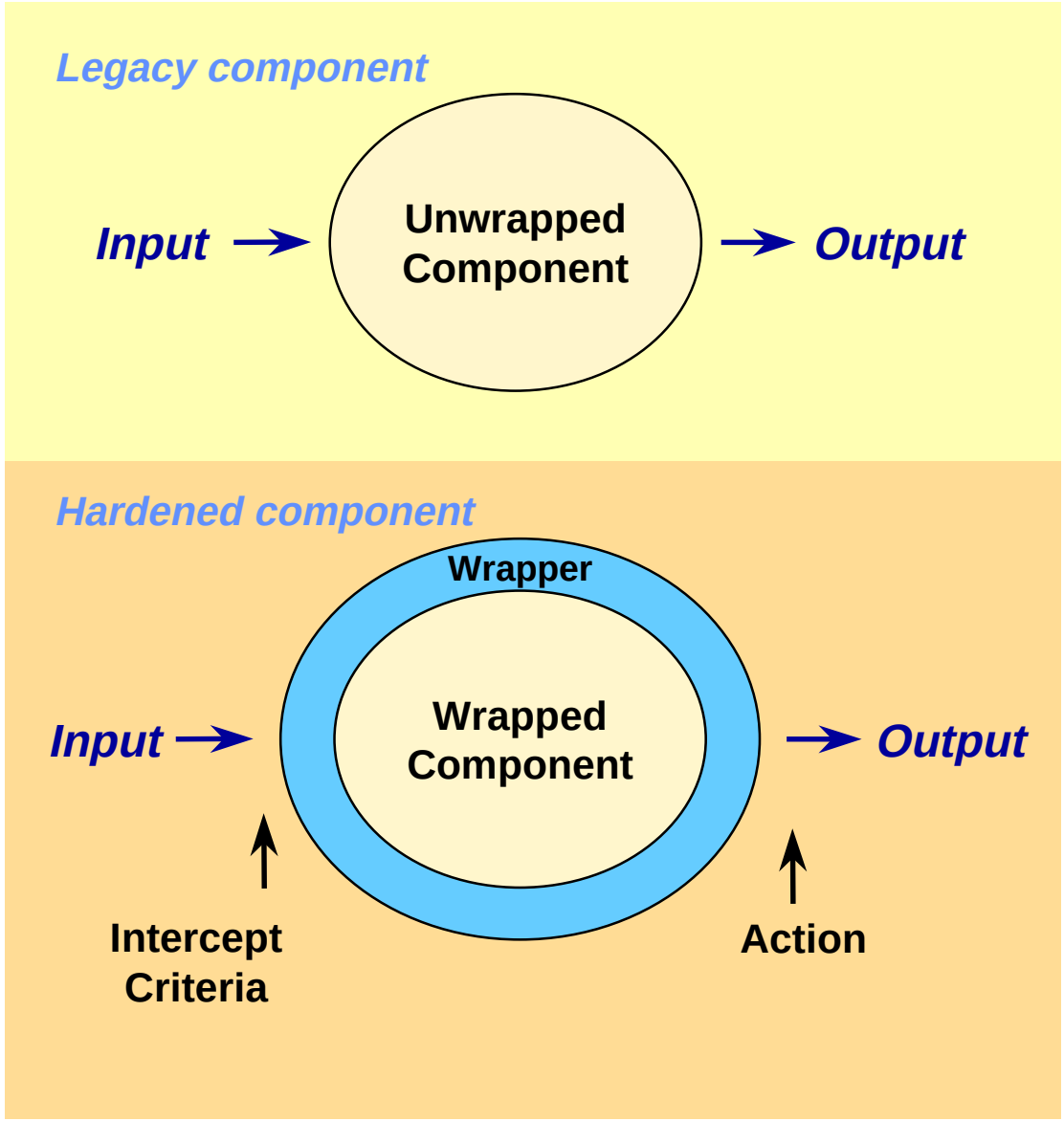
Challenge:
Authenticate name/address transactions





Challenge:
Protect the exchange of routing tables

Using Wrappers to Harden Software Components

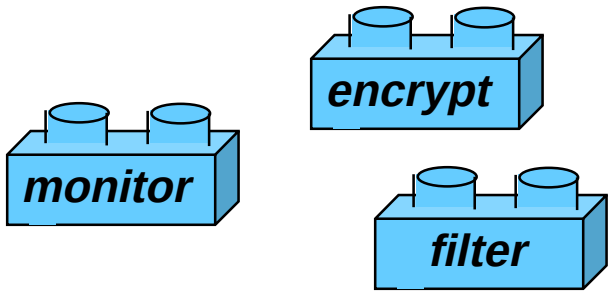


Plug-in wrapper functions:

- Monitoring and management
- Filtering, signatures, encryption, access control
- Replication for fault tolerance

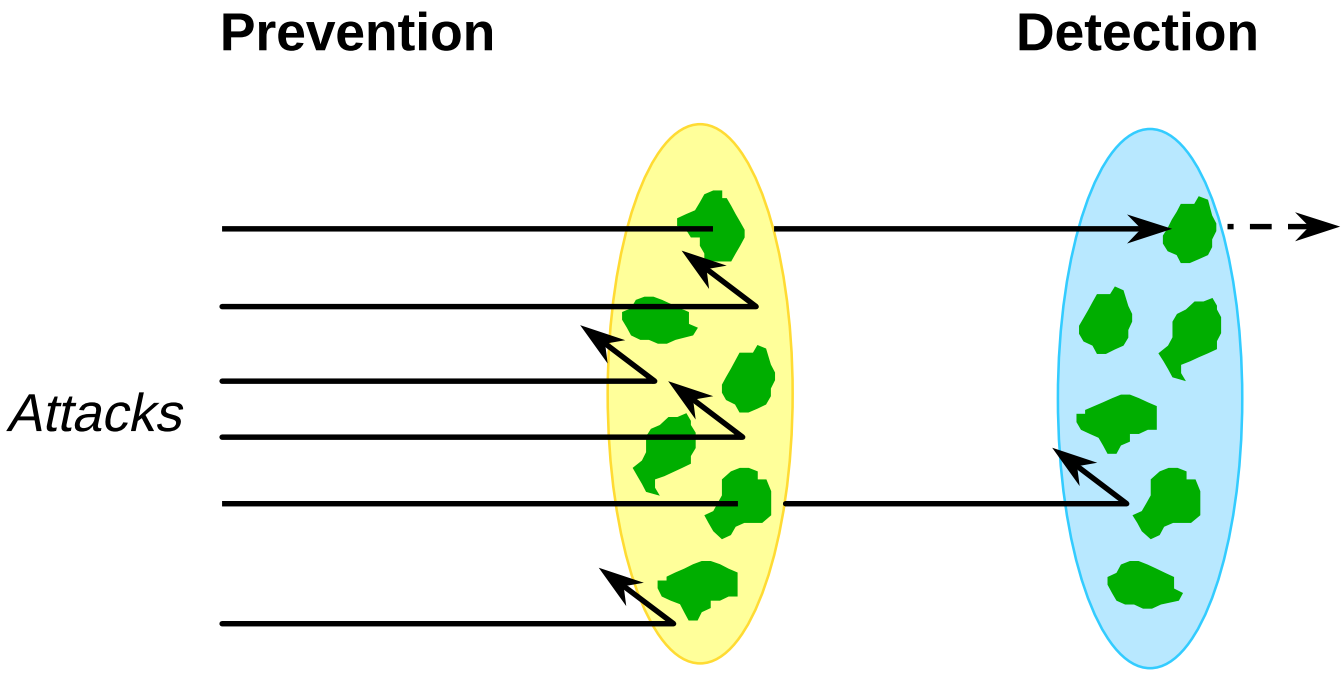
Automated wrapper generation

- Toolbox of survivability modules
- Tools for evaluating the strength of components



Toolkit of plug-and-play wrapper modules

Meshing Prevention and Detection



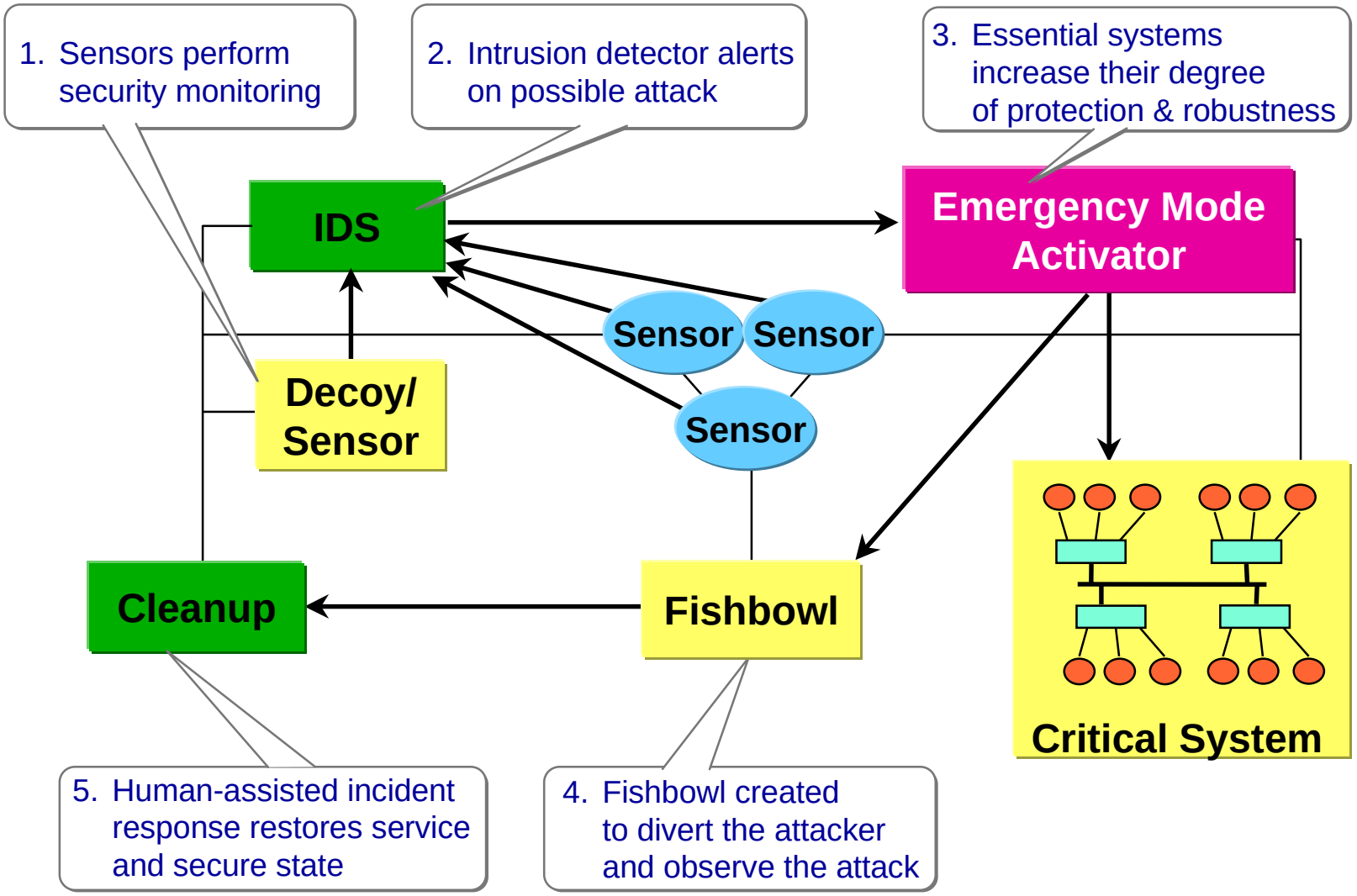
Prevent What You Can

- Firewalls
- End-system security services
- Know where holes are

Detect Residue

- Intrusion detection – attack signatures
- Detect suspicious/unusual activity
- Auto-respond eventually

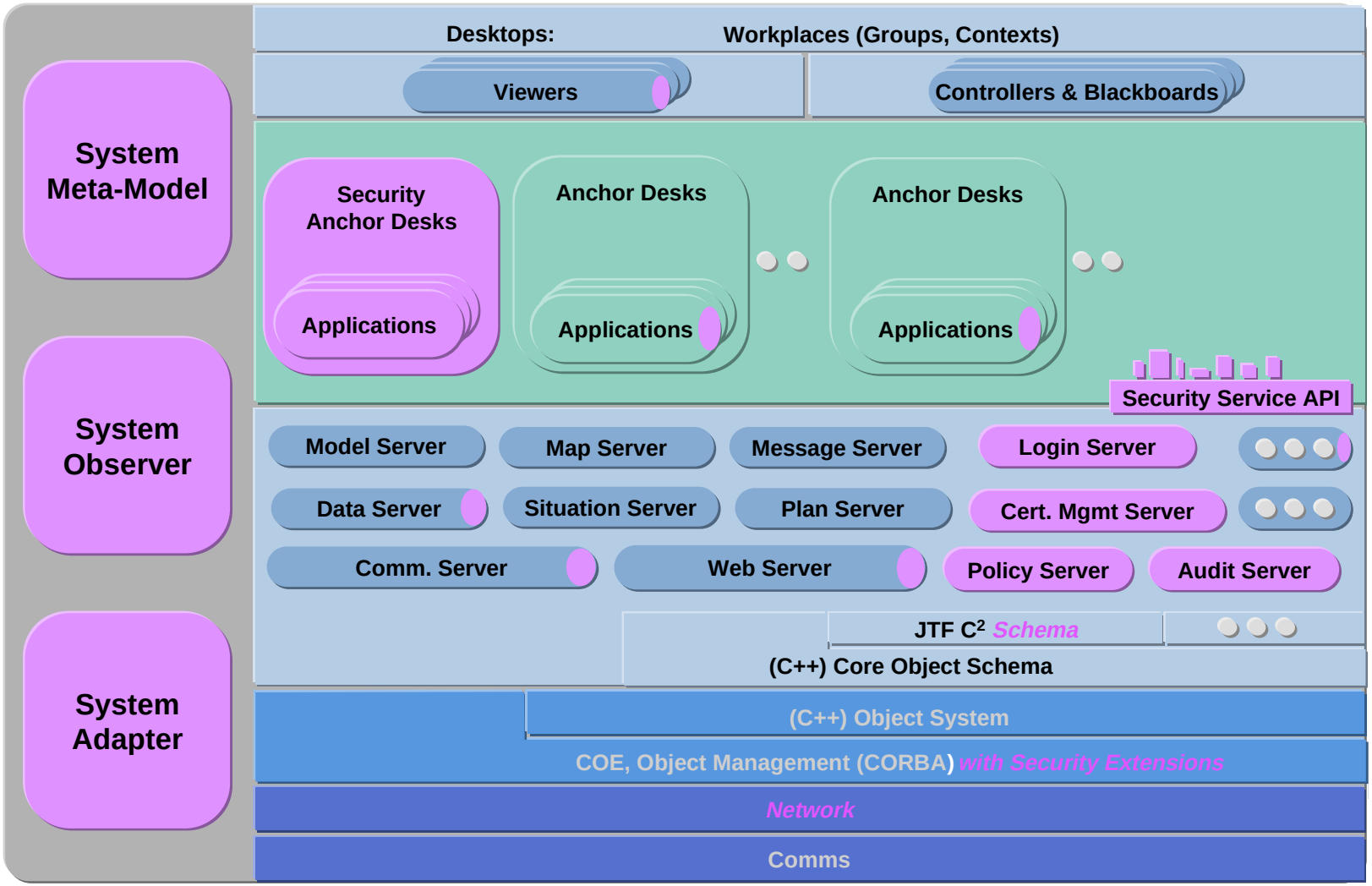
Intrusion Detection and Response



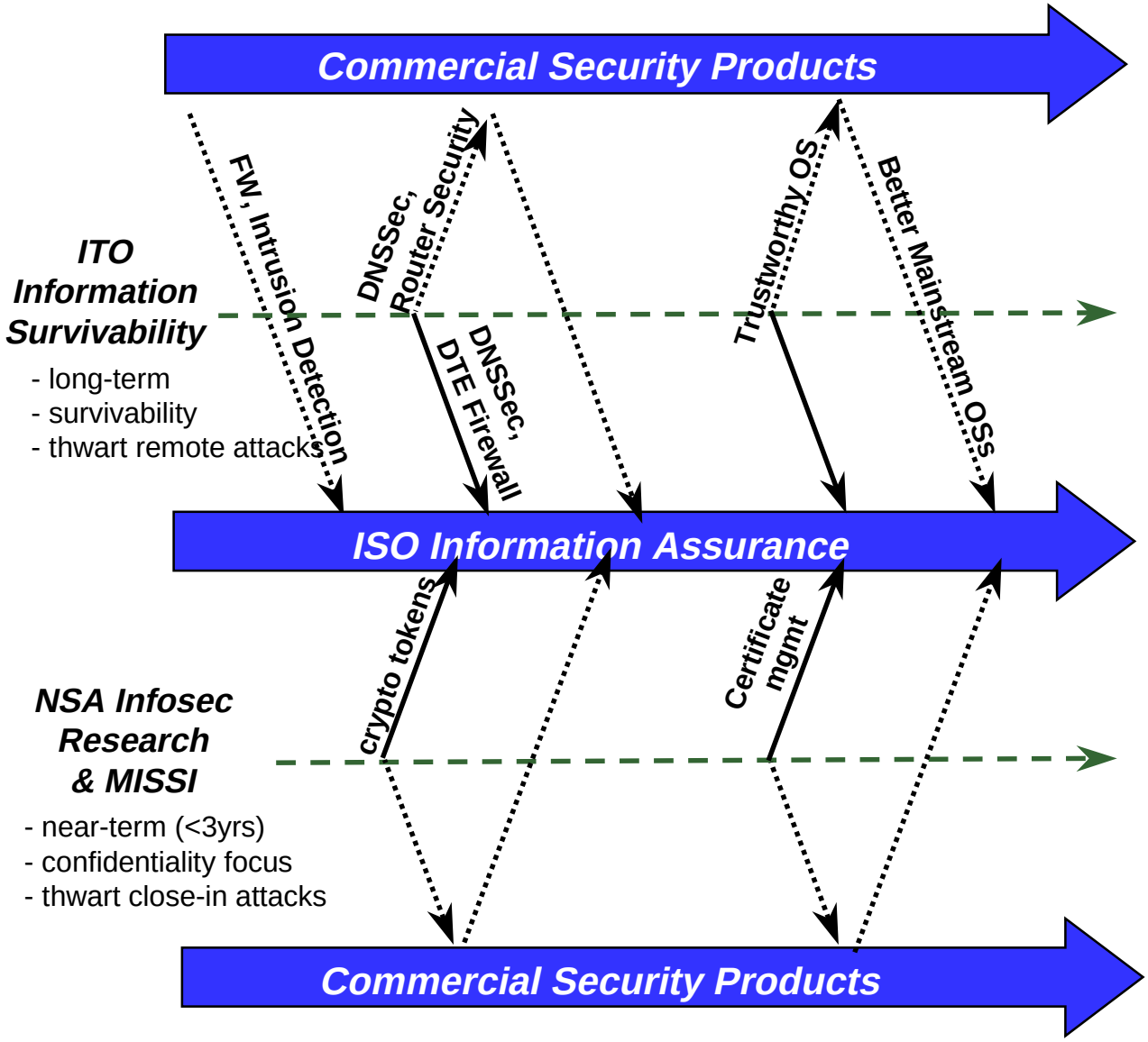
Constituent Technologies

- **IDIP, Intrusion Detection and Isolation Protocol**
- **SNS, a filtering router (Boeing)**
  - Allows/Blocks datagrams based on source and destination host and service (i.e., FTP, Telnet, HTTP, etc.) requested.
- **MIDS, an intrusion detection system (UC Davis)**
  - Examines the network for unusual/unexpected actions (e.g., datagrams, connections, file names, or user names).
- **FWTK, an application layer firewall (TIS)**
  - Allows/Blocks connections based on source and destination host and service (i.e., FTP, Telnet, HTTP, etc.) requested
- **DC, a prototype Intrusion Discovery Coordinator (Boeing)**
  - Collects & displays trace requests / audits from IDIP participants.

Putting it All Together: Extended ISO Reference Architecture



Architecture & Testbed Schedule



Near-term ITO insertion:

- DTE access control and policy specification tools
- Continuous Kerberos v6
- Secure DNS
- Authenticated OSPF
- Robust Flick IDL compiler
- Instrumenting net tool
- Adage authorization server
- Third party key escrow procedure and key release policy language

Long term ITO insertion:

- Secure Access Wrappers for DB, OS, Java
- Traffic analysis countermeasures
- Key release policy engine
- Trustworthy OS technology
- Trustworthy compilers
- Analysis tools to recognize anomalies, attack patterns and vulnerabilities

Recent Accomplishments

• Evaluation Testbed for Intrusion Detection Research Prototypes

AFRL and MIT/LL are developing a realistic simulation network where intrusion detection prototypes will be evaluated using real attacks mixed with normal network traffic for the first rigorous, objective, and repeatable evaluation of competing approaches. False alarm rates and probability of detection for existing and new attacks will be measured

• Specification of Common Intrusion Detection Framework (CIDF) Published

The CIDF framework will allow a variety of network components to work together to detect and respond to network intrusions. The CIDF standardization timetable calls for a revised draft of the specification to be submitted to the Internet Engineering Steering Group (IESG) in December 1998

• StackGuard Compiler Prevents Buffer-Overflow Attacks

Programs compiled with StackGuard, developed at OGI, are are not vulnerable to buffer overflow attacks. No source code changes are required, and executables are binary-compatible with existing operating systems and libraries

• Demonstration of Generic Software Wrappers for Protecting COTS Systems

TIS has developed a wrapper specification language and a UNIX kernel-resident wrapper prototype system structured for migration to the Sun Solaris or NT COE platform. The prototype intercepts all system calls and controls both privileged and non-privileged programs. TIS demonstrated wrappers that control administrative privileges, add access control, and provide encryption

• Successful Demonstration of Intruder Detection and Isolation Protocol (IDIP)

IDIP allows cooperative exchange of information about intrusions by network components using in order to isolate and cut off attacks. Boeing's concept demonstration successfully detected and isolated 10 attacks on the demonstration environment

What Will the Products of the Current Program Be?

- **Prototype implementations of components**
  - **Barriers to Penetration**
    - OS & Router Software; Wrapper Generation Toolkits
  - **Intrusion Detection and Response**
    - Intrusion Detection Algorithms & Software,
      Intrusion Detection / Isolation Protocol, Alertable Firewalls
- **Extensions to AITS (DARPA-DISA) reference architecture**
- **Testbed of extended architecture**
  - Incorporating component outputs
  - Red Team exercises and analysis of results

When Will We Get Them?

- Prototype Component Implementations
  - Barriers to Penetration — FY 99
  - Intrusion Detection and Response — FY 99
- Extended Architecture — FY 98
- Testbed — FY 99 - 00
- Transfer to ACTDs — FY 01
- DoD Impact (first generation) — FY 02 - 04
- Inherent Survivability — FY 00 - 04

Transition of Current IS Program Assets

Survivability of Large-Scale Systems	
• detection of intrusions/suspicious events	**Transition to ISO**
• reactive infrastructure elements (e.g., firewalls)	**Transition to ISO**
• damaged systems redirect resources	**SAFER**
• artificial diversity	**Continue**
• common intrusion detection framework	**Commercialization**
High Confidence Networking	
• protection for current network technologies	**Commercialization & DISA**
• security for active nets and NGI	**NGI, Active Nets**
Wrappers and Composition	
• barriers to attack for legacy systems	**Transition to ISO**
• assessment of security	**Declare victory**
High Confidence Computing	
• security for next-generation OS	**Quorum**
• fault tolerance and real time OS	**Transition to SC-21**
• policy-neutral access control	**Transition to ISO**

The Problem:

We are under attack!

- DISA estimates that there are 250,000 attacks on DoD computer systems every year
- Computer attacks against US systems are up 22% from 1996 to 1997, according to a survey by the Computer Security Institute and the FBI
- **Many successful attacks are not detected**
  - **Intruder makes surreptitious use of penetrated system**
  - **Intruder performs intelligence gathering/theft of data**
  - **Intruder plants malicious code, perhaps for future use**
  - **Intruder may alter data**
- **Our critical systems need to provide continuous correct operation in situations in which they are successfully attacked**

Long-Term Strategy

- Strong Barriers to Penetration
  - Hardened networks and software
- Intrusion Detection
  - Local capability
- Information Assurance Architecture
  - Integrate technologies into systems solutions
- Strategic Intrusion Assessment
  - Distinguish national scale attacks
- Intrusion Tolerant Systems (partially)
  - Maximize the residual capability